ISSN:0975-9646

Foolproof Security for KeyStrokeBiometrics

M. IndraSena Reddy, K. Subba Reddy, V. Uday Kumar

School of Computer science and Engineering,
R.G.M. C.E.T, Nandyal,
Kurnool (Dt), A.P, India-518 501

Abstract— Now-a-days we are facing the majority of crimes related to security issues and these areas due to the leakage of passwords or illegal authentication. At one end, there is a continuous and tremendous improvement in the lifestyle of Humans while at the other end; the technological crimes are increasing rapidly. As there is a problem, there must be a solution. The need for a compromising technology which can be adopted is highly imperative. Technologies capable of identifying each person uniquely need to be developed. The only powerful solution for the problem of illegal authentication is Biometrics. This paper provides an overall idea of Biometrics , the typical Biometric Model, an overview of the Biometric techniques and focuses mainly on Keystroke Biometrics which is easy to implement and can provide fool proof security based on the effectiveness of the algorithm.

Key Words: Authentication, Keystroke biometrics, security, FAR, FRR.

I. INTRODUCTION

As per the saying "**NECESSITY IS THE MOTHER OF INVENTION**", the need for a new type of identification and authentication technique has led to the development of Biometrics**. "**Biometrics is an automated method of recognizing a person based on a physiological or behavioral characteristic**.** Biometrics refers to the physiological or behavioral characteristics of a person to authenticate his/her identity [1]. Due to the increasing demand of enhanced security systems biometric based person authentication system has led to an unprecedented interest of the researchers world-wide. Biometric systems based on a single source of information are called unimodal systems. Although some unimodal systems (e.g. Face, Iris, Palm, Fingerprint) [2], has gotten considerable improvement in reliability and accuracy, they have suffered from enrollment problems due to non-universality of biometric traits, susceptibility to biometric spoofing or insufficient accuracy caused by noisy data [3], Figure 2 shows the sample images of such affected traits. Hence, single biometric may not be able to achieve the desired performance required in real world applications. One of the methods to overcome these problems is to make use of multimodal biometric authentication systems, which combine information from multiple modalities to arrive at a decision. Studies have demonstrated that multimodal biometric systems can achieve better performance compared with unimodal systems. This paper presents score level fusion approach to multimodal biometrics using face and signature modalities. The paper is organized as follows. Approaches to multi-biometric system is discussed Biometric authentication [4], [5] refers to verifying Individuals based on their physiological and behavioral characteristics such as face, fingerprint, hand geometry, iris, keystroke, signature, voice, etc.. Performance (speed and accuracy), acceptability (the willingness of people to use), and circumvention (foolproof) are attributes of biometric systems [6].

Biometric-based solutions are able to provide for confidential financial transactions and personal data privacy. Most systems make use of a personal identification code in order to authenticate the user. In these systems, the possibility of malicious user gaining access to the code cannot be ruled out. However, combining the personal identification code with biometrics provides for a robust user authentication system. Biometrics are of two kinds: One deals with the physical traits of the user (Retinal scanning, Fingerprint scanning, DNA testing etc.,) and the other deals with the behavioral traits of the user (Voice recognition, Keystroke dynamics, etc.) .Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of the economyandourdailylives [7].*THE BIOMETRIC MODEL***:** The biometric authentication system consists: User interface or the biometric reader, Communication Subsystem, The Controlling software, Data storage.

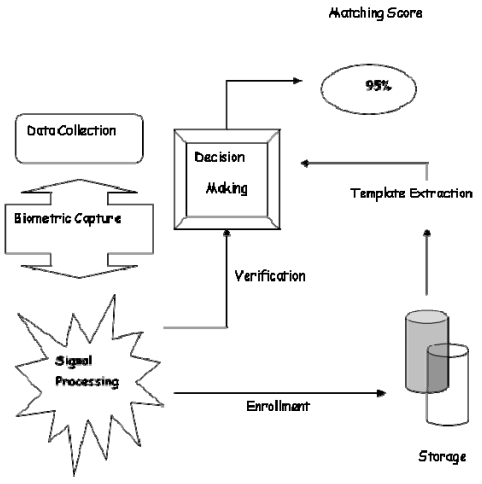


Fig 1: Biometric Model

Biometric system works by taking a number of samples of physiological or behavioral characteristics to produce a reliable template of the user information. The user is verified against a template in the memory, which he claims to be himself and the user is authenticated if the biometric pattern of the user matches with the template. The biometric sample of the person is not stored in the host computer or the controller. So there is no possibility of the others getting it. Moreover, the biometric template of the person is stored in the form of a dynamic binary template with suitable encryption to provide utmost security

B) BIOMETRIC TECHNIQUES:

*1) Fingerprint Verification***:** This is one of the oldest forms of biometric techniques which involves mapping of the pattern of the fingerprint of the individual and then comparing the ridges, furrows, within the template. The fingerprint given to the device is first searched at the coarse level in the database and then finer comparisons are made to get the result.

*2) Iris Recognition***:** In Iris and Retinal scanning, the iris and the retina are scanned by a low intensity light source and the image is compared with the stored patterns in the database template. They are the fastest and the secure form of biometric.

3) Facial Scanning: Facial scanning involves scanning of the entire face and checking of critical points and areas in the face with the template. This method is not completely reliable and so it is used in association with other biometric technique.

*4) Hand and Finger geometry***:** This method uses the data such as length, shape, the distance between the fingers, overall dimensions of the hand and also the relative angle between the fingers. Modern systems use this technique in association with the Fingerprint scanning technique.

5) Voice Biometry: It is proved that the frequency, stress and accent of speech differ from person to person. Voice Biometry uses this concept to solve the problem of illegal user.

*6) Signature Verification***:** This technology uses the dynamic analysis of a signature to authenticate a person. This technology is based on measuring speed, pressure and angle used by the person when a signature is produced.

*7) Keystroke dynamic***:** In this technique, the system analyses the rhythm of typing the password.

II. KEYSTROKE BIOMETRICS

"The keystroke biometrics make use of the inter-stroke gap that exists between consecutive characters of the user identification code. [8]"

When a user types his authentication code, there exists a particular rhythm or fashion in typing the code. If there does not exist any abrupt change in this rhythmic manner, this uniqueness can be used as an additional security constraint. It has been proved experimentally that the manner of typing the same code varies from user to user. Thus this can be used as a suitable biometric. Further, if the user knows before hand about the existence of this mechanism, he can intentionally introduce the rhythm to suite his needs.

III. IMPLEMENTATION DETAILS

As the user logs onto the system for the first time, a database entry is created for the user. He is then put through a training period, which consists of 15-20 iterations. During this time, one obtains the inter-stroke timings of all the keys of the identification code. The inter stroke interval between the keys is measured in milliseconds. The systems' daily routine can be used to serve the purpose. The delay routine measures in milliseconds and the amount of delay incurred between successive strokes can be used as a counter to record this time interval.

The mean and standard deviation of the code are calculated. This is done in order to provide some leverage to the user typing the code. The reference level that we chose is the mean of the training period and the rounded standard deviation is used as the leverage allotted per user. These values are fed into the database of the user. These details can also be incorporated onto the system's password files in order to save the additional overhead incurred.

The mean and the standard deviation can be determined by using the relationship given below

$$mean = \frac{1}{n}$$

$$s\tan dard\ deviation = \sqrt{\frac{2}{n}\sum (x(i) - mean)}$$

Once the database entry has been allotted for the user, this can be used in all further references to the user. The next time the user tries to login, one would obtain the entered inter-stroke timing along with the password. A combination of all these metrics is used as a security check of the user. The algorithm given below gives the details of obtaining the authorization for a particular user. The algorithm assumes that the database already exists in the system and one has a system delay routine available

A) Performance measures:

While considering any system for authenticity, one needs to consider the **false acceptance rate** (**FAR**) and the **false rejection rate** (**FRR**).

The [FAR] is the percentage of unauthorized users accepted by the system.

The [FRR] is the percentage of authorized users not accepted by the system.

An increase in one of these metrics decreases the other and vice versa. The level of error must be controlled in the authentication system by the use of a suitable threshold such that only the required users are selected and the others who are not authorized are rejected by the system. In this paper, standard deviation of the user's training period entry is used as a threshold. The correct establishment of the threshold is important since too strong a threshold would lead to a lot of difficulty in entry even for the legal user, while a lax threshold would allow non-authorized entry. Thus a balance would have to be established taking both the factors into consideration

ALGORITHM

Input : User name, User id, Password.

Output: Registration of a new user (or) Acceptance of a user if registered

(Or) Rejection of an unregistered user.

```
Main ()
{
If (User==New)
{Read (User);                    // Getting User name, User_id, Password
Read (Inter-stroke gap);         // Time interval between consecutive characters
    Add user (database);         // Add the User to the database
    User count =1;  }
Else if (User==Training)
{Read (User);
```

```
Read (Inter-stroke gap);
If (Check (User, Password))
{If (User count<15)
{Update ( User count);    //  User count = User count +1
Add (Inter-stroke gap);   }
Else if (User count ==15)
{Update (User count);
Add (Inter-stroke gap);
Calculate Mean (M), Standard deviation (S.D);    }
 }
   }
Else if (User==Existing)
{   Read (User);
Read (deviation);
If (Check (User, Password, deviation))
        Login;
Else
Exit (0);    } }
```

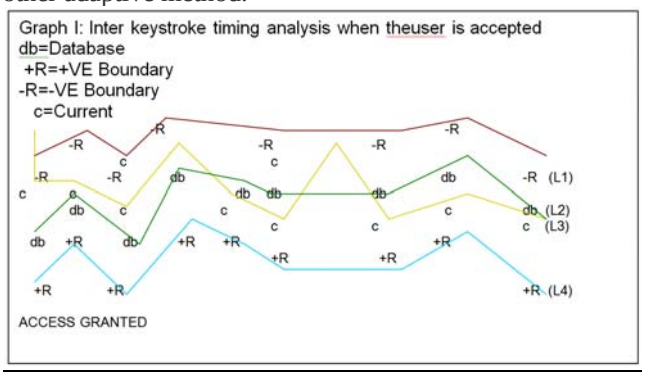
B) Analysis of inter-keystroke timing of user code:

A graph is plotted between keystrokes and keystroke timing. The 'X' axis indicates the number of inter-keystrokes and negative 'Y' axis indicates the inter-keystrokes timing in milliseconds.

1) User accepted:

The graph I show the inter-keystroke timing analysis when the user is accepted. Here it can be easily seen that when the user is authentic or when he types in his normal rhythm, the user automatically comes into the predefined ranges. The current inter-keystroke timing lies around the database inter-keystroke timing, thereby providing adequate amount of predefined ranges. FAR and FRR can be reduced to a treat extent so that only the legal user gets access to the system. The **+R boundary** and **–R boundary gives** the desired range so that only the legal user gets access.

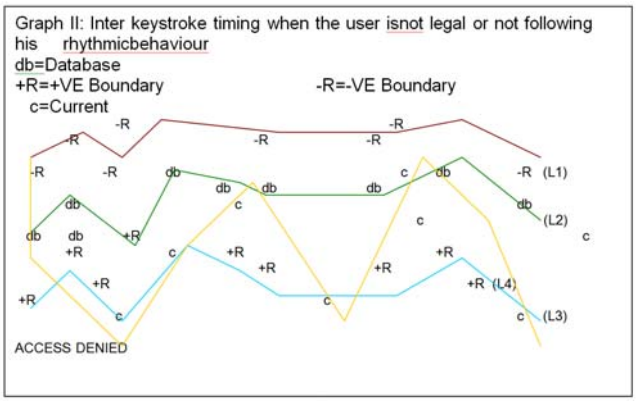
In the graph, the **line (L3)** indicates the current pattern of typing the access code on the keyboard; the **line (L2)** indicates the keystroke pattern according to reference level and the **line (L1)** and **(L2)** indicates the positive and the negative ranges. The ranges can be decided by the standard deviation method, which is used here for analysis or any other adaptive method.



2). User hasn't accepted:

Graph II indicates inter-keystroke timing when the user is not legal or not following his rhythmic behavior of typing the access code. It can be easily noticed when the user is not legal, his typing pattern in the access code is not at all into the predefined ranges.

A biometric system which relies only on a single biometric identifier is often not able to meet the desired performance requirements. Identification based on multiple biometrics represents an emerging trend. This system takes the advantage of the capabilities of each individual biometric and overcomes the limitations of individual biometric. This multi biometric system operates with an admissible response time.



C) Applications:

1) BIOMETRIC BANKING: Banks have been experimenting with keystroke Biometrics for ATM machine use and to counteract the credit card frauds. The smart card or the credit card may be incorporated with the biometric information. When a user inserts his card for verification, the biometric sample of the person can be verified precisely and if it is identically the person is authenticated. The advantage of this system is that the user can enjoy the facilities offered by the Bank along with utmost security.

2) INTERNET SECURITY: If the password is leaked out, the computer or the web server will not be able to identify whether the original user is operating the computer. PCs fitted with biometric sensors can sense the biometric template and transmit it to the remote computer so that the remote server is sure about the user in the computer.

3) BIOMETRIC SMART CARDS: Biometric technologies are used with smart cards for ID systems applications specifically due to their ability to identify people with minimal ambiguity. A biometric based ID allows for the verification of **"who you claim to be"** (information about the card holder stored in the card) based on **"who you are"** (the biometric information stored in the smart card), instead of, or possibly in addition to, checking **"what you know"** (such as passwords).

D) Constraints In Keystroke Biometrics:

A question that arises with any technology is that **"Does this technology have any constraints?"** The answer to this question is that, "It purely depends upon its implementation mechanism". In Keystroke biometrics, the person being authenticated must have registered their bio-identity before it can be authenticated. Registration processes can be extremely complicated and very inconvenient for users. This is particularly true if the user being registered is not familiar with what is happening. The problem for the operator is that the right person will be rejected occasionally by what might be presented as a

'foolproof' system. Both the FAR and the FRR depend to some extent on the deviation allowed from the reference level and on the number of characters in the identification code (Password). It has been observed that providing a small deviation lowers the FAR to almost NIL but at the same time tends to increase the FRR. This is due to the fact that the typing rhythm of the user depends to some extent on the mental state of the user. So, a balance would have to be established taking both the factors into consideration.

E) ***Solution:***

The performance measure of Keystroke biometrics purely depends on User psychology, i.e., the user's particular temperament; understanding and current state of mind can have a dramatic impact on real system performance. If a user is not happy about using the biometric device, he is likely to be consistent in using it, potentially producing a much larger than the average error rate. Conversely, if a user is intrigued and enthusiastic about using the device, he is likely to use it as intended, be more consistent and enjoy 8relatively low error rates. Since this is the case, clearly we should aim for well educated (in terms of the system) users who have good quality reference templates and are happy with the overall system concept and its benefits.

IV. CONCLUSION:

Keystroke Biometrics offers a valuable approach to current security technologies that make it far harder for fraud to take place by preventing ready impersonation of the authorized user. Even if the unauthorized user discovers the access code, he cannot get access to the system until and unless he also knows the rhythm. Also, the typing rhythm can be self-tuned by the user to suit his needs. As the keyboard has duplicate keys, the typing rhythm also depends whether the user is a left-handed person or a right-handed person. **Positively Keystroke Biometrics will replace the entire traditional security systems in the future.**

REFERENCES:

[1] Jain A.K., Ross A. AndPrabhakar S. (2009) *IEEE Transactions on Circuits and Systems for Video Technology*, 14, 4-20.
[2] Chander Kant, RajenderNath (2009) *International Journals of Biometric and Bioinformatics*, 3 (1), 1- 9.
[3] Jain A.K., Ross A. (2004) *Communications of the ACM*, 47, 34-40.
[4] A. K. Jain, R. Bolle, and S. Pankanti, Eds., *Biometrics: Personal Identification in Networked Society*. Norwell, MA: Kluwer, 1999.
[5] D. Maltoni, D. Mao, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*. New York: Springer-Verlag, 2003.
[6] J. L. Wayman, "Fundamentals of biometric authentication technologies,"*Int. J. Image Graph.*, vol. 1, no. 1, pp. 93–113, 2001.
[7] S. Singh, "The Code Book", Doubleday, 1999.
[8] Exploring Biometrics: Seeing the UnseenA paper By Neil F. JohnsonSushilJajodia George Mason University